SYSTEM AND METHOD FOR DELIVERING ENCRYPTED INFORMATION IN A COMMUNICATION NETWORK USING LOCATION IDENTITY AND KEY TABLES

ABSTRACT OF THE DISCLOSURE

Access to digital data is controlled by encrypting the data in such a manner that, in a single digital data acquisition step, it can be decrypted only at a specified location, within a specific time frame, and with a secret key. Data encrypted in such a manner is said to be geo-encrypted. This geo-encryption process comprises a method in which plaintext data is first encrypted using a data encrypting key that is generated at the time of encryption. The data encrypting key is then encrypted (or locked) using a key encrypting key and information derived from the location of the intended receiver. The encrypted data encrypting key is then transmitted to the receiver along with the ciphertext data. The receiver both must be at the correct location and must have a copy of the corresponding key decrypting key in order to derive the location information and decrypt the data encrypting key. After the data encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect secret key, the decryption will fail. If the sender so elects, access to digital data also can be controlled by encrypting it in such a manner that it must traverse a specific route from the sender to the recipient in order to enable decryption of the data. Key management can be handled using either private-key or public-key cryptography. If private-key cryptography is used, the sender can manage the secret key decrypting keys required for decryption in a secure manner that is transparent to the recipient. As a consequence of its ability to manipulate the secret keys, the sender of encrypted data retains the ability to control access to its plaintext even after its initial transmission.